Massachusetts Emergency Support Function 17

CYBERSECURITY

Responsible Agencies

Lead Coordinating Agencies

Executive Office of Public Safety and Security (EOPSS)

Massachusetts Emergency Management Agency

Massachusetts National Guard

Massachusetts State Police

Commonwealth Fusion Center

Executive Office of Technology Services and Security (EOTSS)

Supporting Agencies and Organizations

Massachusetts Department of Public Utilities (DPU)

Department of Homeland Security, Office of Cyber Security and Communications

Department of Defense, Cyber Crime Center

Federal Bureau of Investigation

Federal Emergency Management Agency

United States Secret Service (USSS)

National Cybersecurity and Communications Integration Center (NCCIC)

Multi-State Information Sharing and Analysis Center (MS-ISAC)

Other sector-specific Information Sharing and Analysis Centers (ISACs)

Internet Service Providers

MIT - Cybersecurity at MIT Sloan

IBM Security

RSA Security

1.0. INTRODUCTION

1.1. Purpose

Massachusetts Emergency Support Function 17 (MAESF-17), Cybersecurity, provides a framework for coordination and cooperation across agencies before, during, and after a cyber-related emergency or disaster affecting, or having the potential to affect, the Commonwealth in a significant manner. This coordination and cooperation is intended to enhance the ability of public and private sector stakeholders to prevent, respond to, protect against, mitigate, and recover from cyber related emergencies and disasters and their potential cascading impacts.

1.2. Scope

This annex is applicable to state agencies and departments, as well as affiliated MAESF-17 partners, with cyber incident related roles, responsibilities, and/ or response requirements as outlined in this annex. It describes the framework for partners to:

- Interface with one another, other state agencies, other ESFs, the private sector, and the federal government in establishing and maintaining situational awareness regarding cyber emergencies and disasters;
- Interface with one another, other state agencies, other ESFs, the private sector, and the federal government in preventing, protecting against, mitigating, and responding to cyber emergencies and disasters.
- Access relevant subject matter expertise regarding a potential or ongoing cyber incident
- Assist the State Emergency Operations Center (SEOC), including its Command and General Staff, and other ESFs in understanding technical and operational issues as they relate to actual or potential impacts of cyber emergencies and disasters, including secondary consequences, and in the development of priorities and objectives for the response to a cyber emergency or disaster.

This annex supports and does not supplant existing cyber-related local, state, or federal plans, policies, directives, or executive orders. It is not intended to be a tactical or operational plan for responding to cyber incidents. Rather, it establishes coordination and cooperation mechanisms and a framework to facilitate the development of collaborative or agency-, organization-, or sector-specific prevention, protection, mitigation, response and recovery actions and plans.

2.0 SITUATION AND ASSUMPTIONS

2.1. Situation

The advent of networked technology has spurred innovation, cultivated knowledge, and increased economic prosperity. However, the same infrastructure that enables these benefits is also vulnerable to malicious activity, malfunctions, human error, and acts of nature. Significant cyber incidents are occurring with increased frequency, impacting public- and private-sector infrastructure located in Massachusetts, the United States, and around the world.

While the vast majority of cyber incidents can be handled under existing plans and policies, those that have, or threaten to have, significant impacts on an agency or organization, critical infrastructure, the economy, or delivery of essential services may require a higher level of coordination amongst stakeholders.

2.2. Planning Assumptions

- This annex is not intended to supplant existing cyber-related local, state, or federal plans, policies, directives, or executive orders.
- This annex is not a tactical or operational plan for responding to cyber incidents or attacks.
- Cyber incidents may take a number of different forms: an organized cyberattack, an exploit such as a virus or worm, a natural disaster with significant cyber consequences, or other incidents capable of causing extensive damage to critical cyber infrastructure.
- Cyber incidents can occur at any time with little or no warning, may quickly overwhelm public- and private- sector resources, and result in secondary consequences that threaten life safety, property, critical infrastructure, the economy, and/or the ability to deliver essential services.
- Cyber incidents may not be associated with specific geographical areas and may lack an easily identifiable signature.
- Cyber incidents may impede communications necessary for coordinating response and recovery actions.
- While owners and operators of critical infrastructure systems can and should take precautions to protect their systems prior to the occurrence of a cyber incident, it is reasonable to assume that some owners/operators may have failed to, or are unable to, do so.
- Most cyber infrastructure is owned and operated by the private sector. Effective response to and recovery from a cyber incident will require cooperation and coordination between the public and private sectors.

- Rapid identification, robust information sharing, and coordinated investigative and response/remediation activities may limit the impacts of a cyber incident.
- Not all cyber emergencies will require standing up the State Emergency Operations Center (SEOC), or require immediate actions to be taken, even if MAESF-17 has been activated.
- The state has resources and expertise that can be used to supplement local and private sector efforts. Federal assistance may be requested to support state and local efforts if an incident exceeds state and local capabilities.
- Depending on the magnitude of the incident, resources from other states or the federal government may not be available for use in Massachusetts for as long as 72 hours after a cyber incident is detected.

3.0. CONCEPT OF OPERATIONS

3.1. General

Certain agencies and organizations have significant authorities, roles, responsibilities, or capabilities required for the response to and recovery from cyber incidents. The following agencies, designated in this plan as *lead coordinating agencies*, will have primary responsibility for the coordination of ESF-17 activities:

- EOPSS
- MEMA
- MANG
- MA State Police
- Commonwealth Fusion Center
- EOTSS

MAESF-17 Supporting Agencies/Organizations will play a supporting role and will be brought into MAESF-17 operations by the Lead Coordinating Agencies, as needed.

The SEOC, when activated, is organized and operates under the Incident Command System. When the SEOC is activated, MAESF-17 will fall within the Operations Section and report through a chain of command to the SEOC Operations Section Chief.

3.2. Notification

MAESF-17 Lead Coordinating Agencies may become aware of actual or potential cyber emergencies that are causing, or may cause, significant impacts to life safety, property,

critical infrastructure, communications, critical institutions, transportation, the economy, delivery of essential services, or the well-being of the state, and for which there may be a need for enhanced coordination and collaboration among stakeholders charged with responding to a cyber emergency. Should this occur, the Lead Coordinating Agency may reach out to MEMA Operations via MEMA's 24/7 communications center. MEMA will contact the other Lead Coordinating Agencies to set up an initial MAESF-17 meeting or conference call to discuss and assess the situation and potential next steps. As appropriate, Supporting Agencies/Organizations, or other agencies/organizations, and other ESFs, may be invited to participate in this initial meeting or call. The focus of this initial meeting/call will be on:

- Gaining an initial understanding of the cyber emergency, including establishing facts and assumptions to the extent possible.
- Assessing ongoing or potential impacts of the cyber emergency, providing analysis of the potential extent and duration of the incident, and identifying requirements for consequence management.
- Determining whether there may be a need for the state to help share information or coordinate resource support to public and/or private sector entities regarding protection against a cyber threat, to facilitate restoration of disrupted network services/systems, or to facilitate the response to secondary and cascading impacts of a cyber incident.
- Prioritizing response actions, including the activation of MAESF-17 and the SEOC if needed to facilitate coordination amongst MAESF-17 Lead/Supporting agencies/organizations or manage the response to the incident's cyber and non-cyber impacts.
- Determining whether there may be a need to share non-sensitive preparedness and prevention information with the general public pertinent to the given situation.

3.3. Information Sharing

In order to encourage greater sharing of information, ESF-17 Lead and Supporting Agencies/Organizations will make use of the Traffic Light Protocol (TLP), an established schema to indicate when and how information may be shared, in order to ensure that sensitive information is shared only with the appropriate audiences. Further information about the TLP may be found in Appendix 2.

3.4. Activities

ESF-17 Lead and Supporting Agencies/Organizations should conduct the following actions:

a) Prevention/Protection Actions

- Users of networked systems may prevent cyber incidents by proper usage of networks, systems, and applications in compliance with applicable information security policies.

- Users of networked systems may prevent cyber incidents by creating, implementing, and maintaining policies and procedures to secure networks, systems, and applications.
- Ensure procedures and program/contact information are up-to-date. Discuss lessons identified from incidents and exercises, and explore creative ways to leverage resources.
- Communicate and share information with other Lead and Supporting Agencies/Organizations, and with other agencies/organizations, as appropriate.
- Collaborate with other Lead and Supporting Agencies/Organizations, and others, as appropriate, on prevention/protection/mitigation initiatives.

b) Preparedness Actions

- Participate in regular meetings of MAESF-17 Lead and Supporting Agencies/Organizations, and other stakeholders to review and update this annex.
- Develop and maintain operational plans and procedures, resource directories, and emergency contact lists to support MAESF-17 activities, including response and recovery actions.
- Ensure all Lead and Supporting Agencies/Organizations have at least primary and secondary points of contact, and other pre-designated staff as necessary, to support this annex and SEOC operations.
- Ensure that MEMA's Operations Unit has a current roster of Lead and Supporting Agency/Organization primary and secondary points of contact, and that MEMA's Operations Unit is promptly notified of staff changes.
- Ensure procedures are in place to quickly notify and communicate with primary and secondary points of contact each Lead and Supporting Agency/Organization, and for other personnel who may be called upon to support this plan.
- Ensure that points of contact and support staff of Lead and Supporting Agencies/Organizations who may be called upon to support this annex or SEOC operations are, and remain properly trained on ESF-17 and SEOC procedures and operations.
- Participate in exercises and trainings in order to test, validate, and provide practical experience for ESF-17 personnel on this annex and related procedures.
- Develop coordination mechanisms, strategies, and requirements for post-incident assessments, plans, and activities that are scalable to incidents of varying types and magnitudes.
- Conduct after action discussions of prior MAESF-17 efforts and other studies to improve future operations.
- Develop long-term strategies and plans in coordination with other relevant stakeholders to address key MAESF-17 issues regarding cyber incidents.

- Develop plans, procedures, and guidance delineating appropriate participation and available resources, that take into account the differing technical needs and statutory responsibilities.

c) Response Actions

Initial Response to Cyber Incidents

- Establish facts and assumptions concerning the cyber emergency.
- Assess ongoing impacts of the cyber incident (both cyber- and non-cyber-related), provide analysis of the potential extent and duration of the incident, and identify requirements for consequence management.
- Identify and prioritize response actions.
- Provide appropriate representative(s) to the SEOC as requested to support MAESF-17.
- Monitor and maintain situational awareness and provide relevant and appropriate information to the SEOC Planning Section to facilitate the development of Situational Awareness Statements or other situational awareness products.
- Use available information to plan effective response actions.
- Identify and coordinate response and recovery resources.
- Coordinate MAESF-17 support to other ESFs regarding primary, secondary or cascading impacts. Ensure that other ESFs have an understanding of these impacts and their relationship to potential or actual threats.
- Coordinate with Federal counterparts as needed.
- If the SEOC is activated, track committed resources and provide updates to the MAESF-17 desk at the SEOC, and to the Operations and Planning Sections in the SEOC.
- Prepare and process reports, using established procedures, giving attention to the production of after-action reports.
- Begin to compile recommendations for after-action reports and other reports as needed.

Continuing Response to Cyber Incidents

- Continue to coordinate resources to support requests for assistance and support.
- Conduct ongoing re-assessment of priorities and strategies to meet the most critical needs.
- Coordinate with other MAESFs as appropriate to anticipate projected MAESF-17 needs and/or coordinate appropriate response efforts to primary, secondary, or cascading impacts.
- If the SEOC is activated, provide information to the Planning Section as needed to inform Situational Awareness Statements and the SEOC Roster.

- Draft recommendations for after-action reports and other reports as appropriate.

d) Recovery Actions

- Coordinate replacement and restoration of damaged or destroyed equipment and facilities in the affected areas.
- Coordinate with support agencies to ensure adequate cost accounting measures are being used, and summary reports are generated and shared with the SEOC.
- Coordinate with support agencies to ensure financial tracking of all deployed assets and adequate cost accounting measures are being used. Generate summary reports and share with the SEOC.
- Participate in after-action reviews.

4.0. ROLES AND RESPONSIBILITIES

4.1. MAESF-17 Lead Coordination Agency Responsibilities

a. Executive Office of Public Safety and Security (EOPSS)

- Share information, as appropriate, with Lead and Supporting Agencies/Organizations;
- Convene calls or meetings of Lead Agencies/Organizations to discuss and assess significant cyber incidents or threats, and to discuss next steps and action items, as set forth in this Annex;
- Participate in, and support MAESF-17 activities, including information sharing, coordination with other Lead Agencies/Organizations, staffing the MAESF-17 desk in the SEOC, as appropriate and as set forth in this Annex; .
- Provide strategic guidance and leadership.

b. Massachusetts Emergency Management Agency (MEMA)

- Provide administrative support to Lead and Supporting Agencies/Organizations in maintaining this Annex, and in convening and supporting calls or meetings of ESF-17
- Support MAESF-17 planning and operational activities
- Provide workspace in the SEOC to support MAESF-17 meetings and activations
- Share information, as appropriate, with Lead and Supporting Agencies/Organizations;
- Convene calls or meetings of Lead Agencies/Organizations to discuss and assess significant cyber incidents or threats, and to discuss next steps and action items, as set forth in this Annex;

- Participate in, and support MAESF-17 activities, including information sharing, coordination with other Lead Agencies/Organizations, staffing the ESF-17 desk in the SEOC, as appropriate and as set forth in this Annex;
- Coordinate with Federal partners through FEMA.
- Coordinate state response actions to the consequences of a cyber incident, utilizing the State CEMP as a framework.
- Facilitate the coordination of recovery efforts.
- Facilitate communication and coordination with other entities involved in cyber incidents on a statewide basis by providing:
    - Administrative support
    - Information dissemination
    - Meeting space and/or conference call bridges

c. Massachusetts National Guard

- Share information, as appropriate, with Lead and Supporting Agencies/Organizations;
- Convene calls or meetings of Lead Agencies/Organizations to discuss and assess significant cyber incidents or threats, and to discuss next steps and action items, as set forth in this Annex;
- Participate in, and support MAESF-17 activities, including information sharing, coordination with other Lead Agencies/Organizations, staffing the ESF-17 desk in the SEOC, as appropriate and as set forth in this Annex;
- Provide a conduit for information between DOD and state government.

d. Massachusetts State Police

- Share information, as appropriate, with Lead and Supporting Agencies/Organizations;
- Convene calls or meetings of Lead Agencies/Organizations to discuss and assess significant cyber incidents or threats, and to discuss next steps and action items, as set forth in this Annex;
- Participate in, and support MAESF-17 activities, including information sharing, coordination with other Lead Agencies/Organizations, staffing the ESF-17 desk in the SEOC, as appropriate and as set forth in this Annex; Assist in attributing the source of cyber incidents.
- Provide a conduit for information sharing and intelligence sharing between local, state and federal law enforcement agencies, state government and the private sector.
- Ensure coordination between MAESF-17 and the MSP Homeland Security and Preparedness Division.

e. Commonwealth Fusion Center (CFC)

- Share information, as appropriate, with Lead and Supporting Agencies/Organizations;
- Convene calls or meetings of Lead Agencies/Organizations to discuss and assess significant cyber incidents or threats, and to discuss next steps and action items, as set forth in this Annex;
- Participate in, and support MAESF-17 activities, including information sharing, coordination with other Lead Agencies/Organizations, staffing the MAESF-17 desk in the SEOC, as appropriate and as set forth in this Annex;
- Provide a conduit for information sharing and intelligence sharing between local, state and federal law enforcement agencies, state government and the private sector.
- Provide accurate and timely intelligence products.
- Provide direct analytical support for investigations involving precursor criminal activity.
- Promote awareness of priority intelligence requirements and of indicators of threats to the Commonwealth.

f. Executive Office of Technology Services and Security (EOTSS)

- The Executive Office of Technology Services and Security (EOTSS) is the Executive Branch's service provider for networking, hosting, unified communications, telecommunications, and desktop infrastructure. EOTSS is focused on protecting digital assets and working to enhance the Commonwealth's cybersecurity posture.
- Share information, as appropriate, with Lead and Supporting Agencies/Organizations;
- Convene calls or meetings of Lead Agencies/Organizations to discuss and assess significant cyber incidents or threats, and to discuss next steps and action items, as set forth in this Annex;
- Participate in, and support MAESF-17 activities, including information sharing, coordination with other Lead Agencies/Organizations, staffing the MAESF-17 desk in the SEOC, as appropriate and as set forth in this Annex;

4.2. MAESF-17 Supporting Agency/Organization Responsibilities

- Report to the SEOC as directed. Coordinate with the MAESF-17 desk at the SEOC regarding available MAESF-17 assets to include assets located at headquarters, district, region, or other affiliated offices statewide.
- Commit stakeholder resources as needed.

- Develop written procedures to implement the responsibilities outlined in the Massachusetts Comprehensive Emergency Management Plan (CEMP).

4.3. Other Agencies

Other agencies not explicitly named in this annex may have authorities, resources, capabilities, or expertise required to support MAESF-17 activities. These agencies may be requested to provide support as needed.

5.0. ADMINISTRATION AND LOGISTICS

5.1. Staffing

All agencies with MAESF-17 responsibilities must designate at least one primary and one secondary point of contact to act as liaisons to MAESF-17 and the SEOC. These liaisons should be knowledgeable about the resources and capabilities of their respective agency/organization and have access to the appropriate authorities for committing said resources and capabilities.

5.2. Mutual Aid

The process for requesting mutual aid from entities either within or outside of Massachusetts is described in the "Mutual Aid" section of the State CEMP Base Plan.

5.3. Annex Review and Maintenance

This annex will be updated every two years at a minimum, in accordance with the Emergency Management Program Administrative Policy, and will ensure that appropriate stakeholder input is incorporated into updates. Additionally, the annex will be reviewed following any exercise or activation of the plan that identifies potential improvements. Revisions to this annex will supersede all previous editions and will be effective immediately.

6.0. AUTHORITIES AND REFERENCES

6.1. Authorities

See Authorities section of the State CEMP Base Plan.

6.2. References

- Massachusetts Comprehensive Emergency Management Plan
- Massachusetts Executive Order 144
- Massachusetts Executive Order 476
- Massachusetts General Laws, Chapter 22C, Section 38
- National Cyber Incident Response Plan
- Blueprint for a Secure Cyber Future
- Presidential Policy Directive (PPD) 41, United States Cyber Incident Coordination

APPENDIX 1: CYBER INCIDENT SEVERITY SCHEMA

Incident Level	General Definition
Level 5 **Emergency**	Poses an imminent threat to life safety, the provision of wide-scale critical infrastructure services, or national or state government stability.
Level 4 **Severe**	Likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties.
Level 3 **High**	Likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 2 **Medium**	May impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 1 **Low**	Unlikely to impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 0 **Baseline**	Unsubstantiated or inconsequential event.

APPENDIX 2: TRAFFIC LIGHT PROTOCOL (TLP)